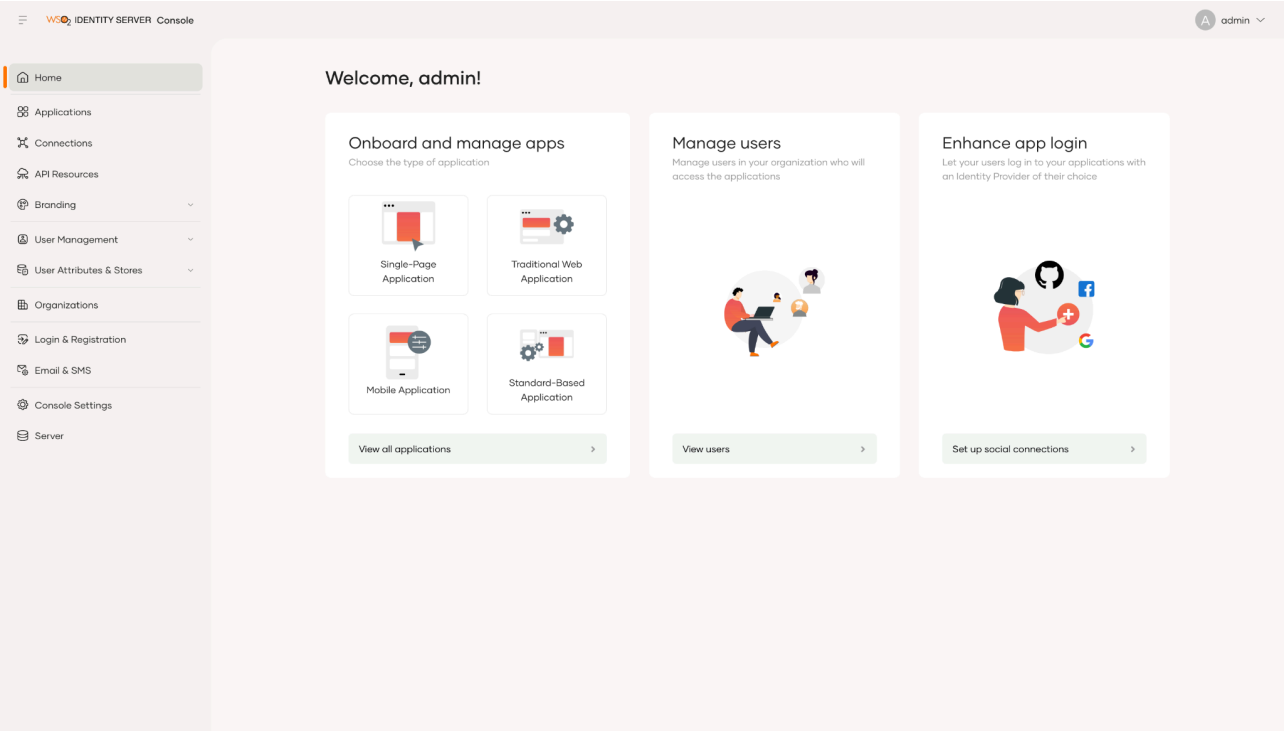
User, Group and Role Management

Introduction

In this tutorial, we are going to try out the User, Group and Role Management in WSO2 Identity Server. This topic involves,

1. managing users, groups, roles.
2. managing permissions associated with roles and groups.
3. assigning users into groups and roles.

These user management tasks can be performed in various ways including using the Console app, using APIs and using My Account.



Lab 01: User Management via Console

Let's create a user and assign the user to a group. And then create a role and assign the role to the group. This way, users will have permissions associated with the roles assigned to the group.

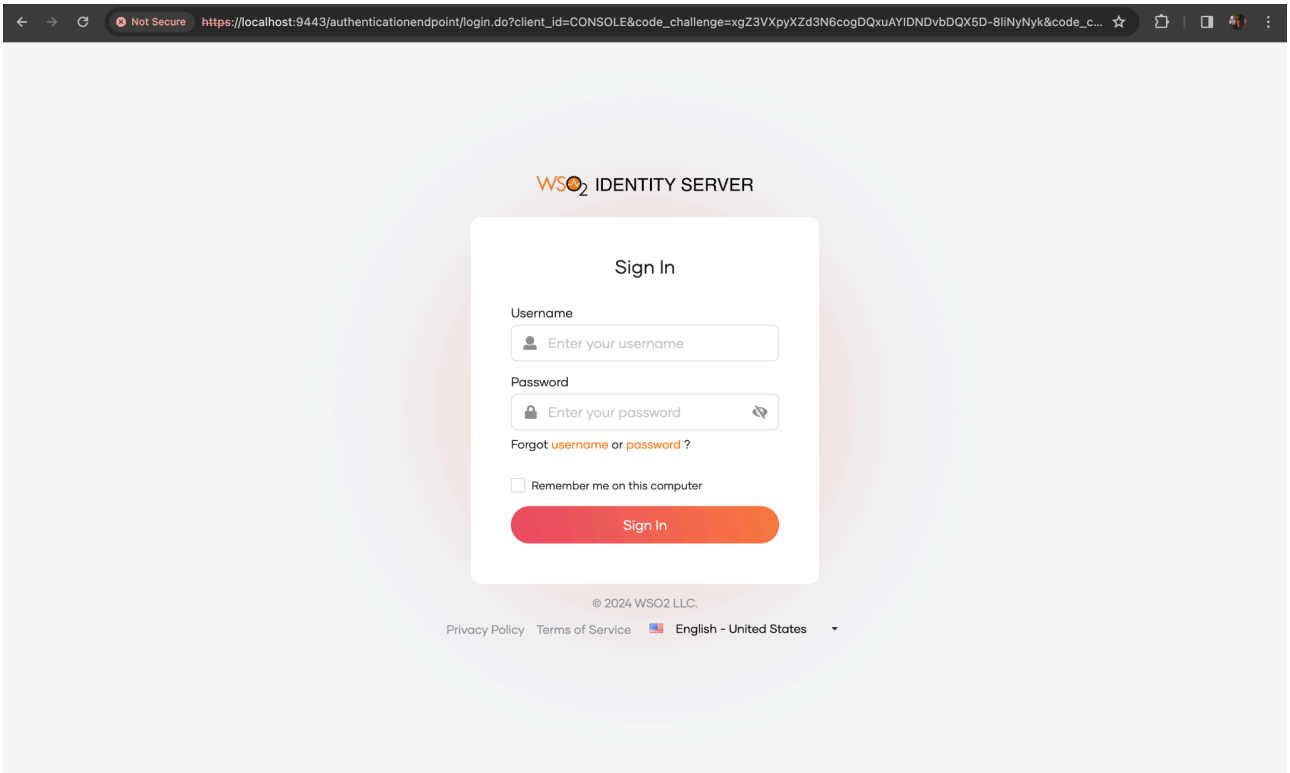
Access Console

To access the Wso2 Identity Server Console, follow these steps:

1. Download the latest version of WSO2 Identity Server from the web site .
2. Please verify that all the system requirements are satisfied.
    - Java version should 11 or 17
3. Navigate to `<IS_HOME>/bin` and start the server by executing either of the following,

    `./wso2server.sh` (Ubuntu , Mac) or **`./wso2server.bat`** run (Windows)

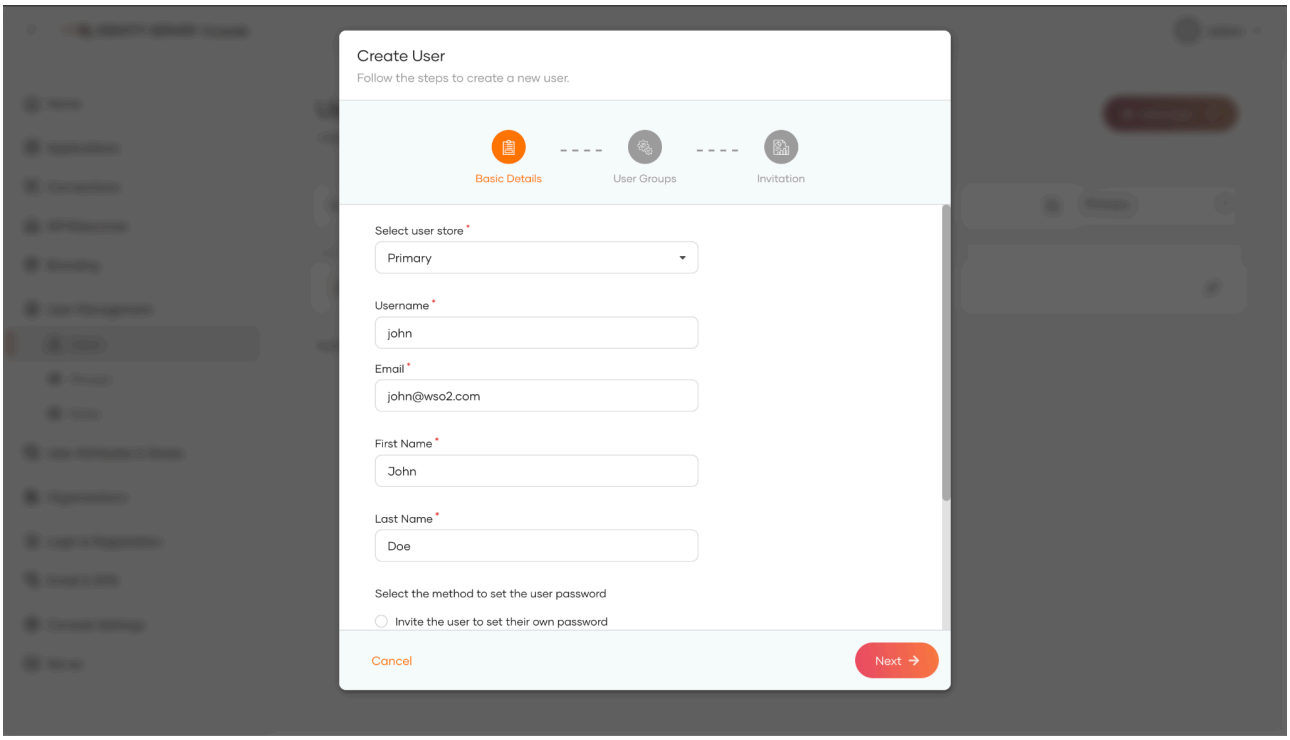
4. Log in to the Console App (https://localhost:9443/console), and enter **admin** as both the username and the password.


Not Secure
https://localhost:9443/authenticationendpoint/login.do?client_id=CONSOLE&code_challenge=xgZ3VXpyXZd3N6cogDQxuAYIDNDvbDQX5D-8liNyNyk&code_c...
IDENTITY SERVER
Sign In
Username
Enter your username
Password
Enter your password
Forgot username or password ?
Remember me on this computer
Sign In
© 2024 WSO2 LLC.
Privacy Policy
Terms of Service
English - United States

Add New Users

To add a new user, follow these steps:

1. Expand the **User Management** menu item, click on **Users**.
2. On the **Users page**, click **Add User** and select **Single User** from the dropdown.
3. In the opened up wizard,
    - Keep **Primary** as the user store.
    - Add the below configuration to the respective fields.
        - Username: **john**
        - Email: **john@wso2.com**
        - First Name: **John**
        - Last Name: **Doe**
    - When you scroll down a bit, you will see 2 options as the method to set the user password. For the simplicity of the guide, select **Set a password for the user** option.
        - When **Invite the user to set their own password** option is selected, an email will be sent to the configured email address and the user will have to goto the link to get to the password setting page. There, the user can add the preferred password.
4. As we selected **Set a password for the user** option add the below password as the user password.
    - Password: **John@1234**



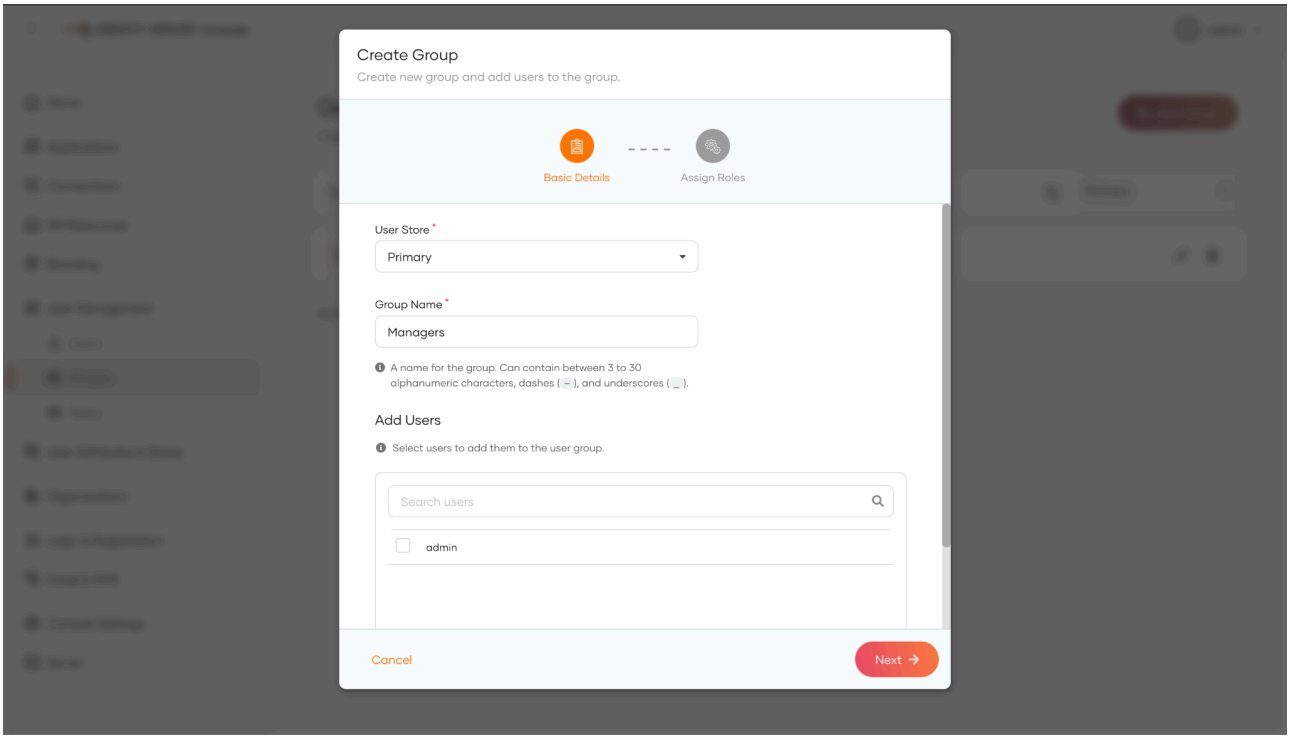
5. Click **Next.**
6. As we have not added any groups yet, skip group selection and Click **Save & Continue**.
7. Click **Close.**

Add New Groups

Group is a collection of users who are managed as a single unit within the organization to streamline assigning permissions and roles.

To add a new groups, follow these steps:

1. Expand the **User Management** menu item, click **Groups**.
2. On the **Groups** page, click **New Group**.
3. Enter **Managers** as the group name.
4. From the list of users, select **john** as a member of the Managers group.
5. Click **Next.**



6. As we have not created any roles yet, skip role selection and Click **Finish**.

Add New User Role

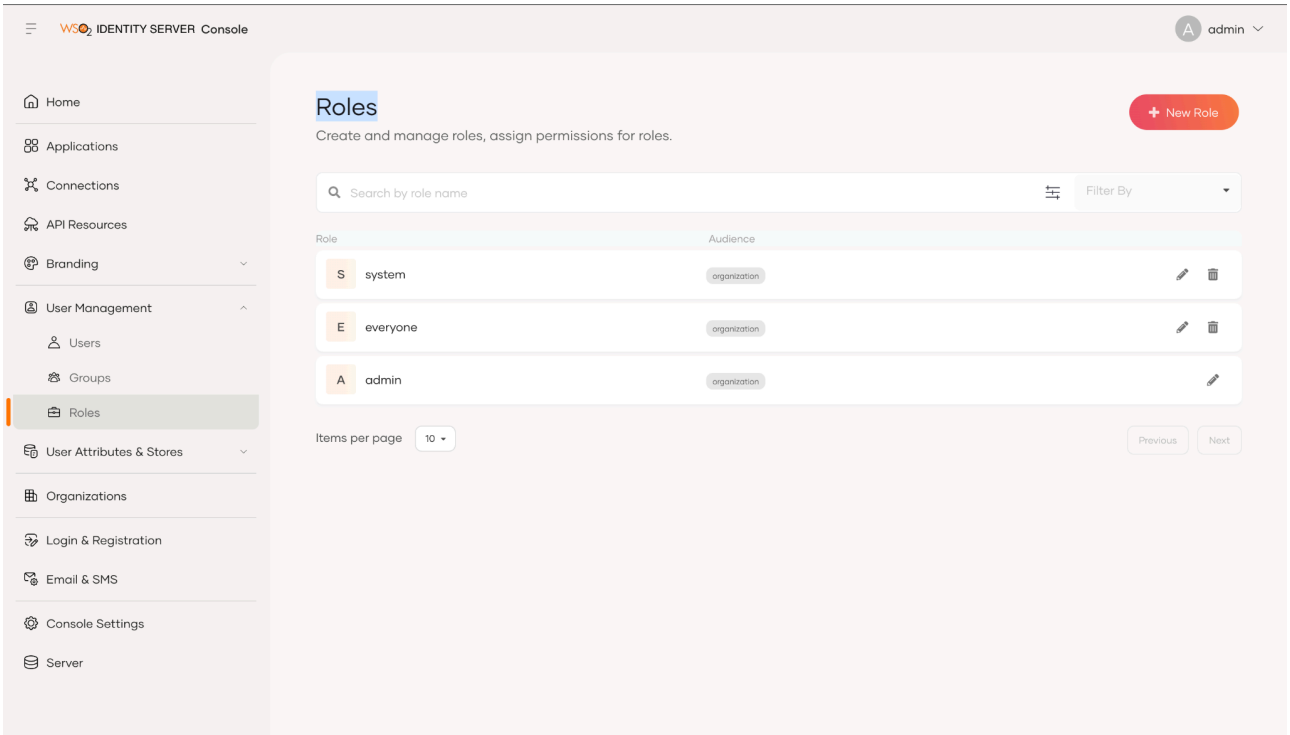
Role represents a set of permissions and responsibilities assigned to a user or group of users within an application, or organization.

Organization Role

Organization roles are defined in the organization level and can be used in the application level when multiple applications use the same access privileges.

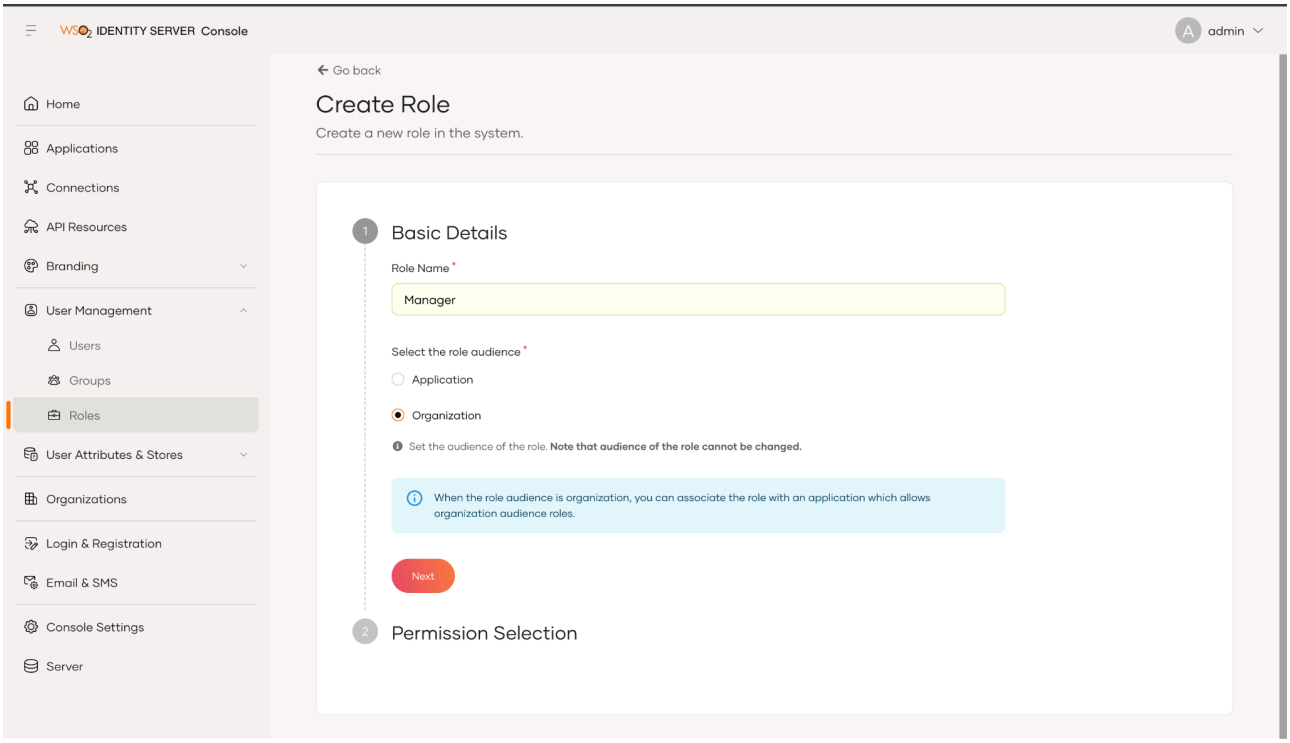
To add a new user role, follow these steps:

1. Expand the **User Management** menu item, click **Roles**.



2. On the **Roles** page, click **New Role**.
3. Enter **Manager** as the role name.

4. Select **Organization** as the role audience.



5. Click **Next** to goto the **Permission Selection** section.
6. Choose relevant scope from the drop down given. (To maintain the simplicity of this section, let's skip the step)
7. Click **Finish**.
8. On the Role page, goto **Groups** tab and click on **Assign Groups** to add groups.
9. From the dropdown, select **Managers** group.
10. Click **Update**.

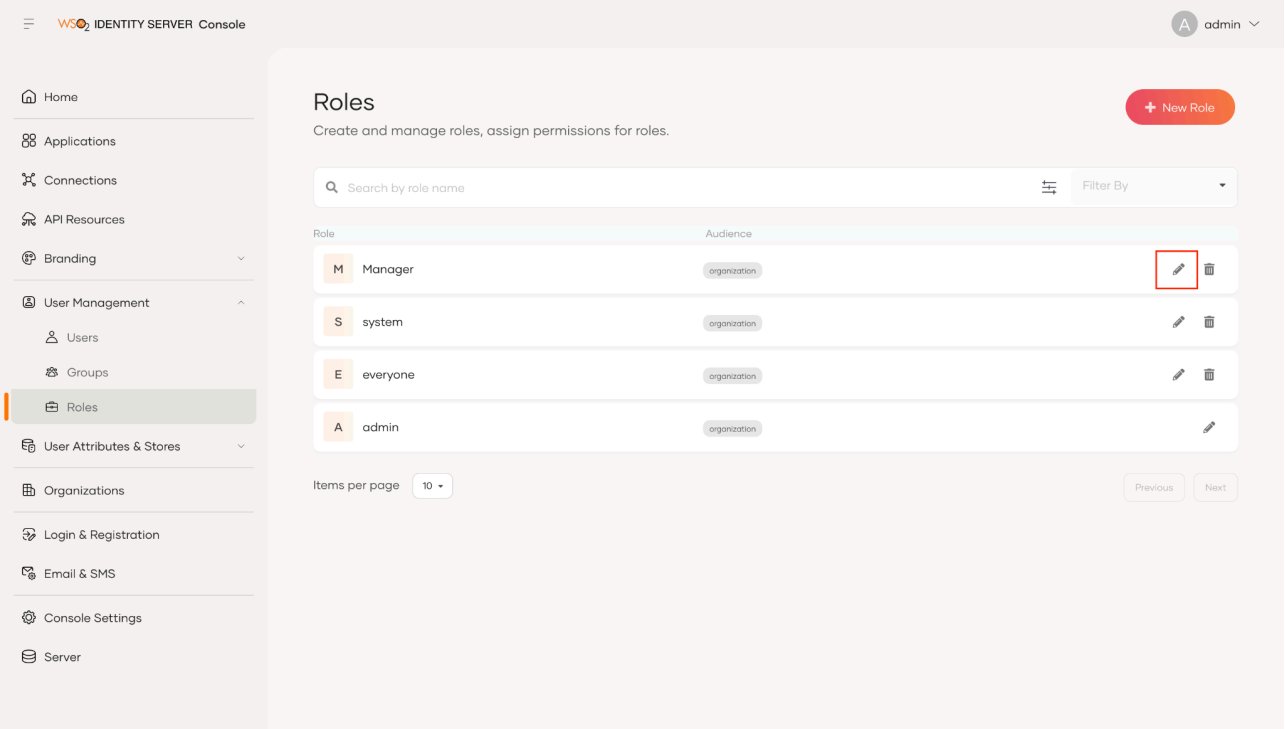
Application Role

These types of roles are tailored to the specific requirements of an application. Further details about application roles such as usage will be discussed in **12. API Authorization** tutorial.

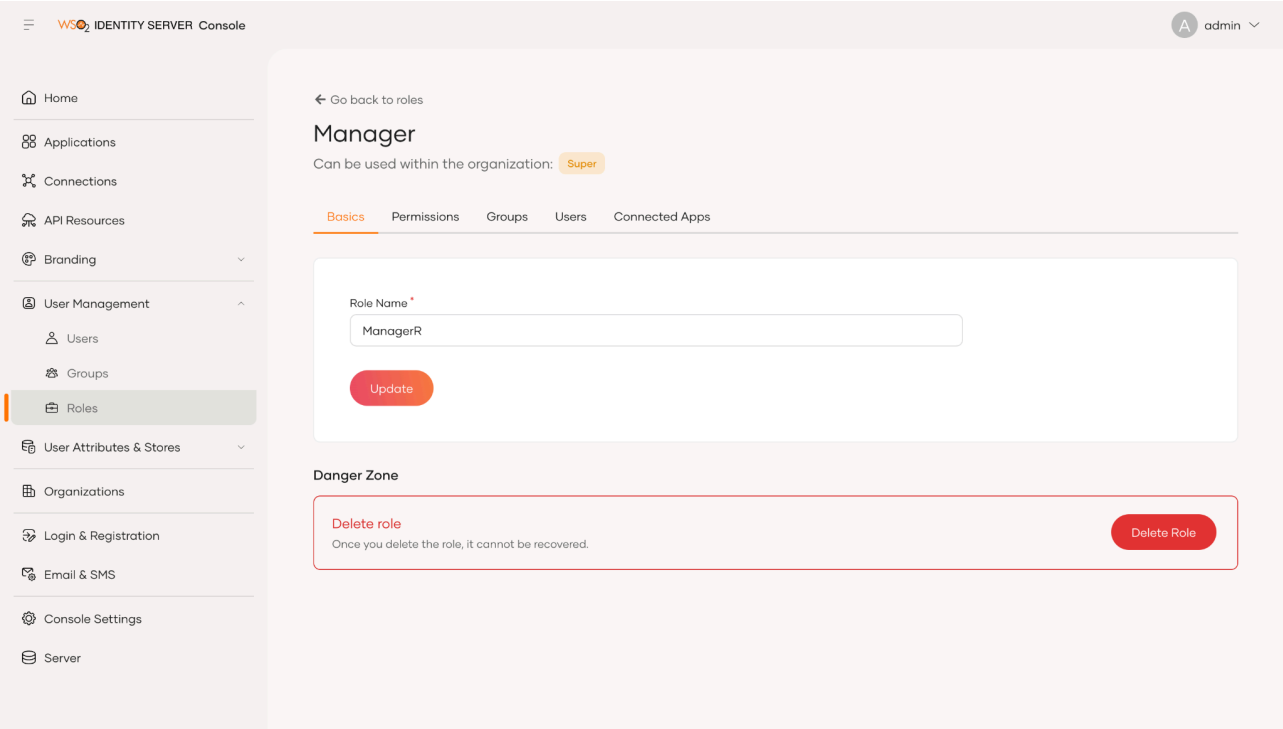
Update Existing User Role

To update the Manager role that you previously added, follow these steps:

1. Expand the **User Management** menu item, click **Roles**.
2. On the **Roles page**, the **Manager** role is displayed in the list of roles.
3. Click on the **Edit** button.



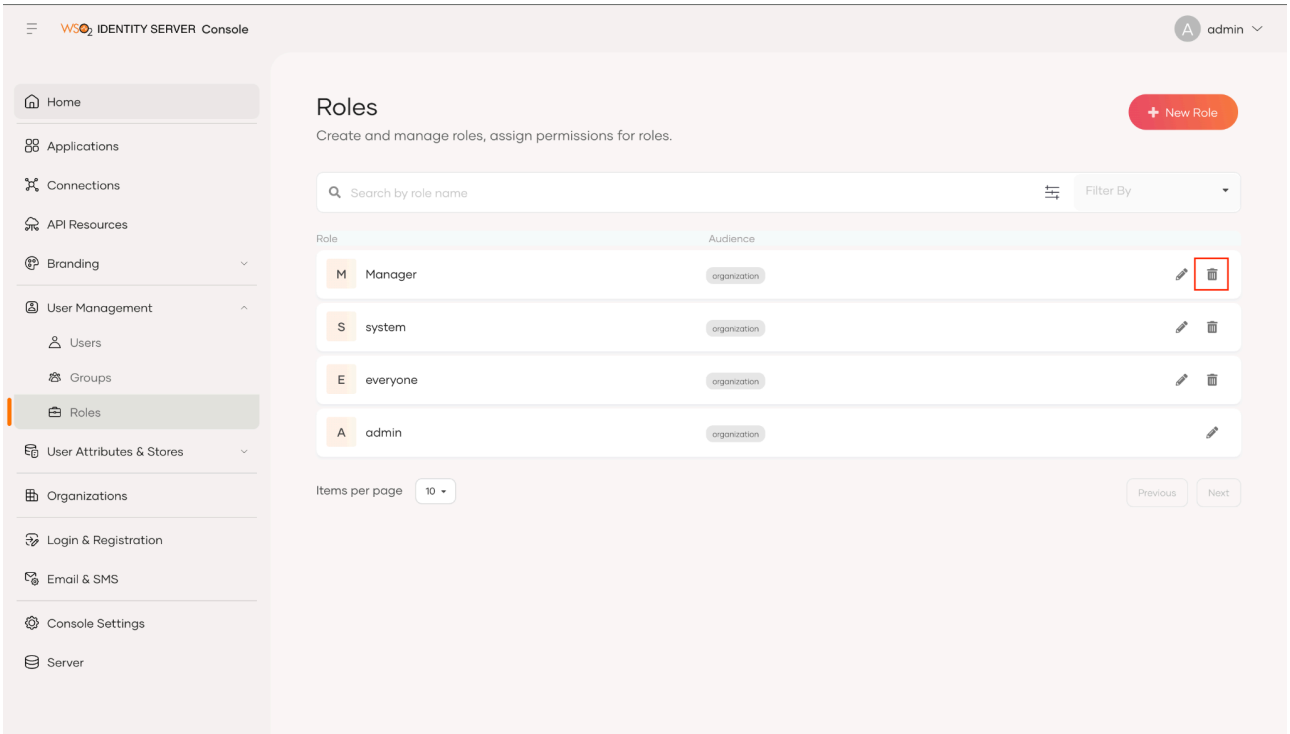
4. Enter a new name in the **Role name** area, and click **Update**.



Delete User Roles

To delete a role, follow these steps:

1. Expand the **User Management** menu item, click **Roles**.
2. Click on the **bin** icon of the relevant role to **Delete role**.


WSO2 IDENTITY SERVER Console
admin
Home
Applications
Connections
API Resources
Branding
User Management
Users
Groups
Roles
User Attributes & Stores
Organizations
Login & Registration
Email & SMS
Console Settings
Server
Roles
Create and manage roles, assign permissions for roles.
New Role
Search by role name
Filter By
Role
Audience
M
Manager
organization
S
system
organization
E
everyone
organization
A
admin
organization
Items per page
10
Previous
Next

Assign Permissions to a User Role

To assign permissions to a specific user role, follow these steps:

1. Expand the **User Management** menu item, click **Roles**.
2. On the **Roles page**, click on the **Edit** button of the **Manager** role displayed in the list of roles.
3. Click on the **Permissions** tab to add a permission.
4. When you expand the drop down of **Select API Resource**, the available API resources are listed as options. By selecting the API resources you will be giving the role to have access to the selected API resources.
5. Select the **SCIM2 Roles API** under **Management APIs** as the **API resource**.
6. After selecting an API Resource you need to select the **level of permissions(scopes)** you want to have for the selected API Resource. ex: view, edit, update, delete
7. Select **View Role and Create Role** as the scope.
8. Click **Update**.

Try It

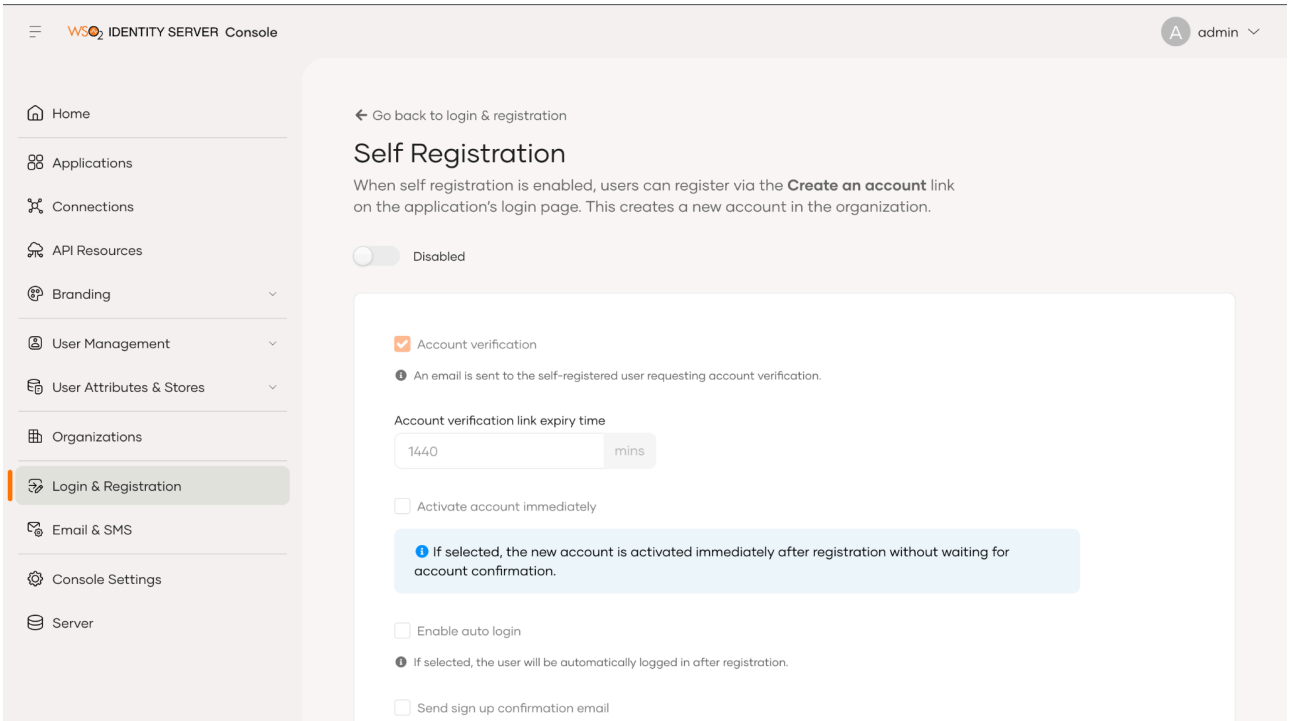
To verify whether the users, role, and group you defined are correctly updated, follow these steps:

1. Expand User Management menu Item and select Groups.
2. Select **Managers** Group.
3. Goto the Users tab.
    - You should see **john** listed as a user.
4. Goto the Roles tab.
    - You should see **Manager** listed as a role.

Lab 02: User Self-Registration via My Account

To learn how a user can self-register via My Account, follow these steps:

1. To enable self user registration in your organization, follow these sub-steps:
    a. On the WSO2 Identity Server Console, go to **Login & Registration** > **User Onboarding** > **Self Registration**.



    b. Toggle the switch to enable self-registration.
    c. Leave the other configurations unchanged.
    d. Click **Update** to save the changes.

2. To send the sign up confirmation email, configure the email server to send emails by following the below steps.
    a. Open the `deployment.toml` file in the `<IS_HOME>/repository/conf` path.
    b. Specify values for the from_address, username, and password parameters in the `[output_adapter.email]` section as shown in the extract below:

```
[output_adapter.email]
from_address="<email>"
username="<email>"
password="<password>"
hostname="smtp.gmail.com"
port=587
enable_start_tls=true
enable_authentication=true
```

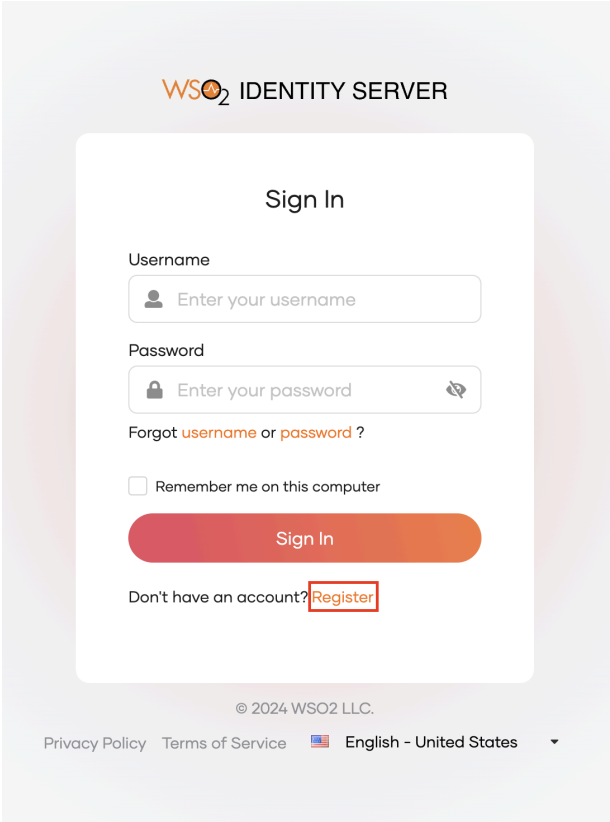
(if you are using a gmail account as the sender, create an App password and use that as the password. If your password contains invalid characters such as “>” , “<” and “&”, enter the password as "<![CDATA[xxxx]]>")

    c. Restart the WSO2 Identity Server.

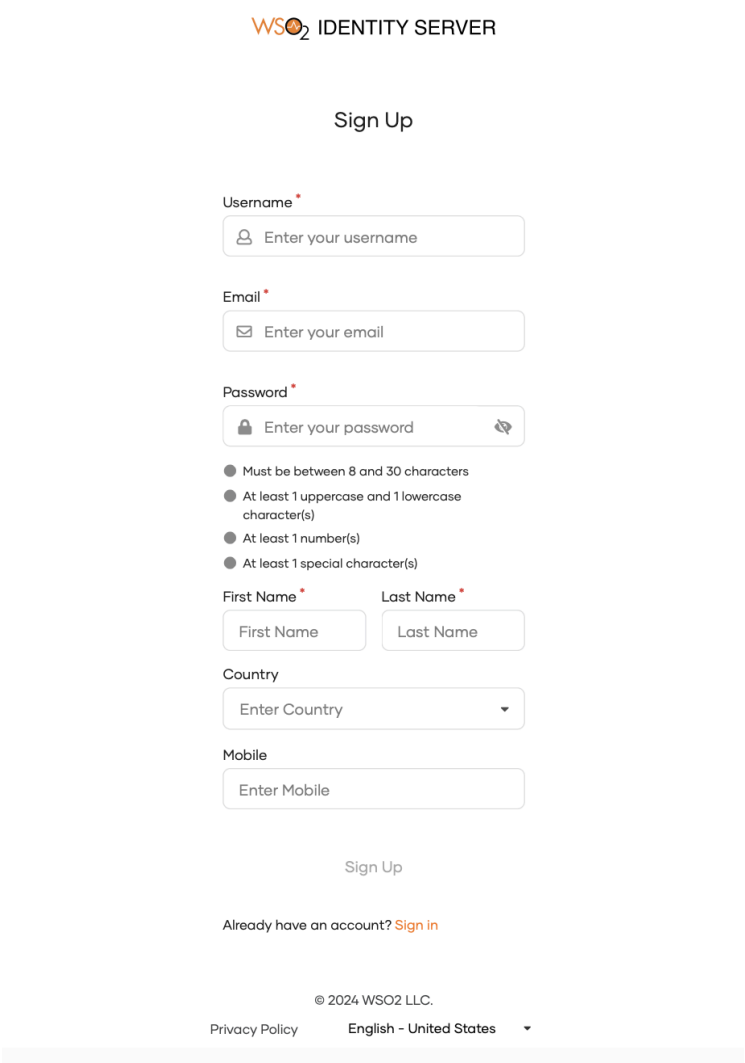
Try It

To verify whether you have successfully enabled self-registration, follow these sub-steps:

1. Access My Account and click **Register**.



2. Click on **Continue with email**.
3. Specify values for the user account.



4. Click **Sign Up**.
5. Check the inbox of the registered email account. You must have received an email to activate the account created. Click on that link to confirm the account.
6. Go to My account and log in using created users credentials. You should be able to log in.

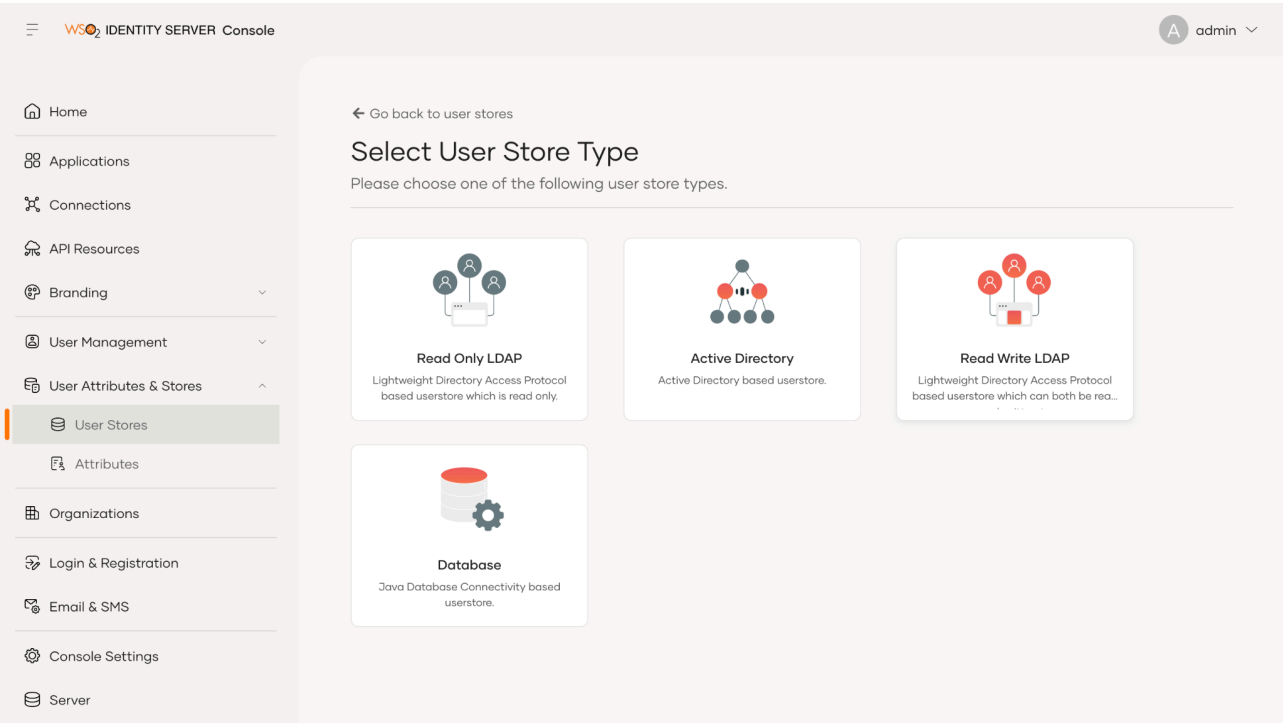
Lab 03: Setting up a Secondary User Store

In this lab, you will set up the Mysql JDBC Database as a secondary user store in WSO2 IAM and connect a user to it.

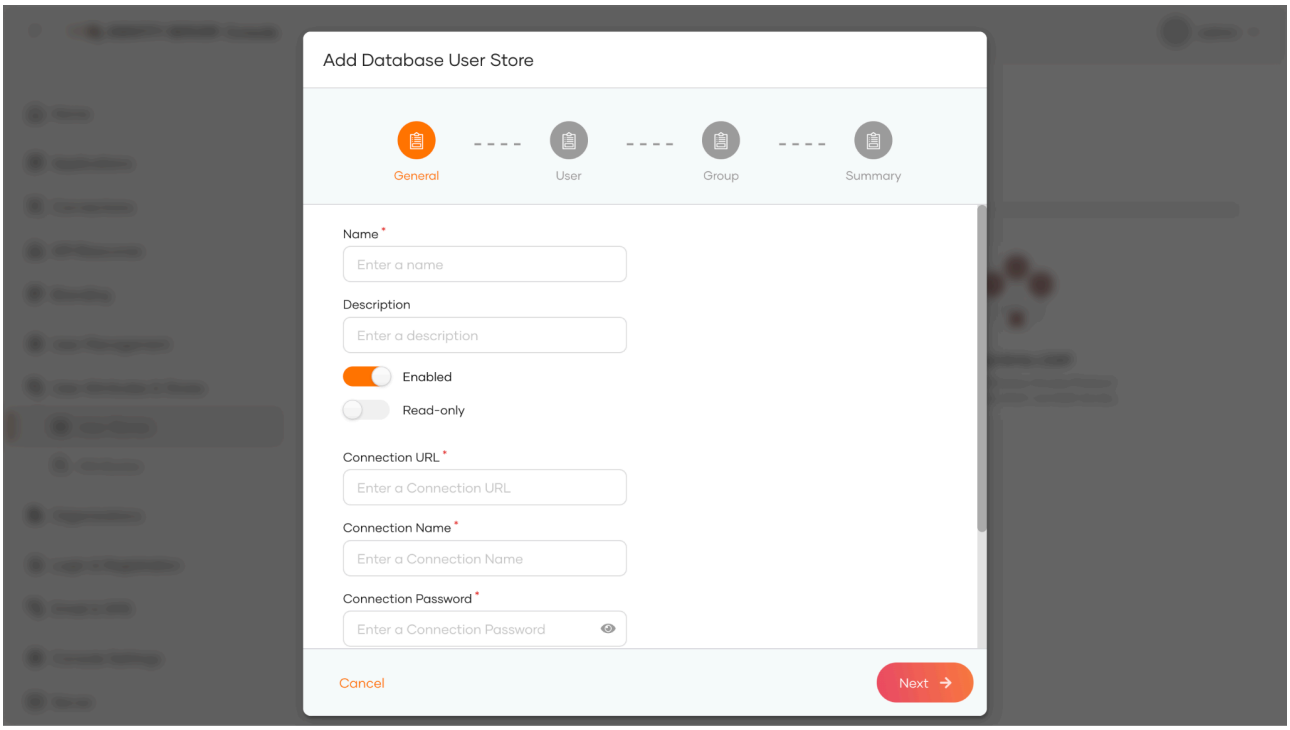
Setting Up

To set up the MySQL-based secondary user store, follow these steps:

1. First Create a Mysql database.
2. Execute `<IS_HOME>/dbscripts/mysql.sql` against the created database to create the database tables.
3. Download the Mysql driver(mysql connector) and extract the zip find to the `mysql-connector-j-<version>.jar` inside the extracted folder.
4. Locate the jar under `<IS_HOME>/repository/components/lib` folder.
5. Restart the WSO2 Identity Server.
6. On the WSO2 Identity Server Console, go to **User Attributes & Stores** > **User Stores**.
7. Click **New User Store** and select the user store type.



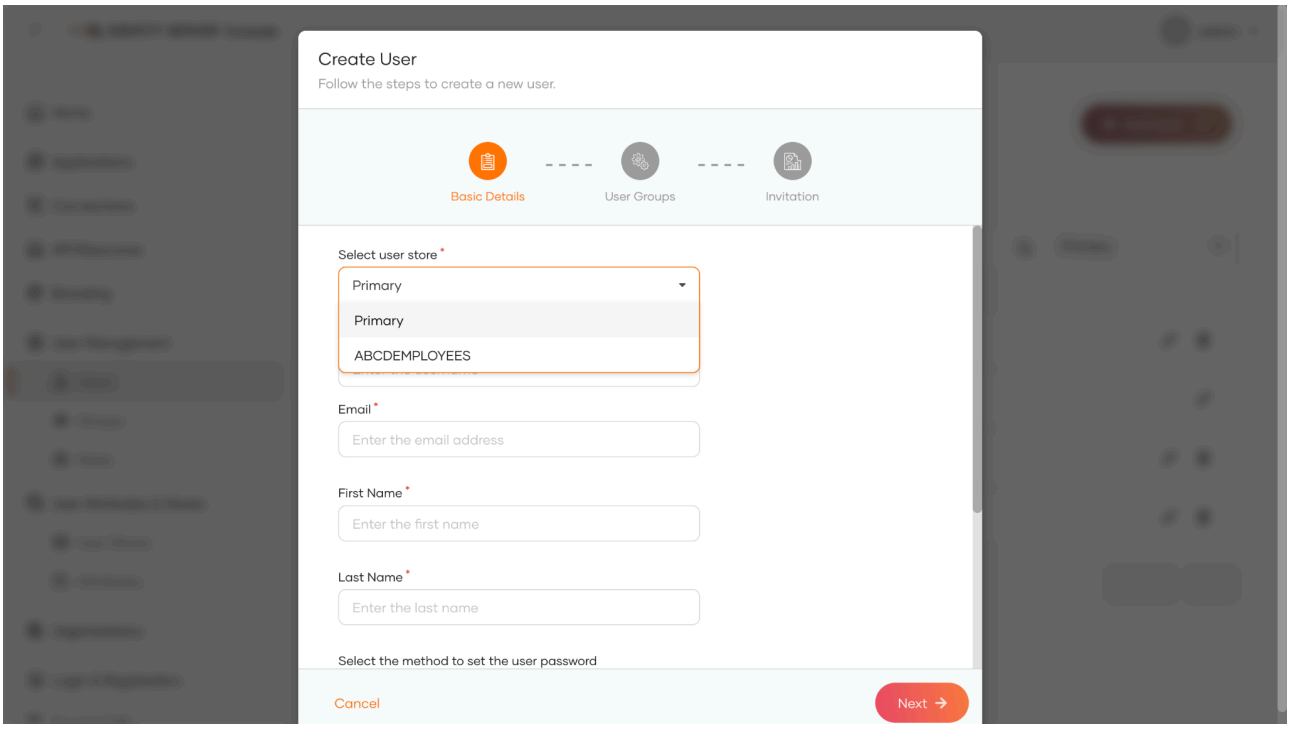
8. Select Database as the option.
9. Enter the below mentioned values for the mandatory fields.
    a. **Name:** ABCDEmployees
    b. **Connection URL:** jdbc:mysql://localhost:3306/{Database_Name}?useSSL=false&allowPublicKeyRetrieval=true
    c. **Connection Name:** Username of the DB User
    d. **Connection Password:** Password of the DB User
    e. **Driver Name:** `com.mysql.cj.jdbc.Driver`
10. To test the connection click on **Test Connection** and verify.



11. Click **Next.**
12. Click **Next** from the User section.
13. Click **Next** from the Group section.
14. Click **Finish**.
15. Refresh the page after a few seconds to check the status. If the new user store is successfully added, it will appear in the user stores page.

Let's try adding a user to the secondary user store

1. On the WSO2 Identity Server Console, go to **User Management** > **Users**.
2. Click on **Add User** and select **Single User.**
3. In the create user wizard, when you expand the **Select user store** dropdown, one should be able to see the user store created.



4. Select the created **ABCDEmployees** secondary user store and fill the relevant information of the user.
5. Now a user is added to the secondary user store.
6. Query the UM_USER table in the MySql database. You will see that the user is created.

```
SELECT * FROM UM_USER;
```